

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED

JAN 27 1999

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)
)
Communications Assistance) CC Docket No. 97-213
For Law Enforcement Act) FCC 98-282

REPLY COMMENTS OF THE
CENTER FOR DEMOCRACY AND TECHNOLOGY

Jerry Berman, Executive Director
James X. Dempsey, Senior Staff Counsel
Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20006
(202) 637-9800
<http://www.cdt.org>

Martin L. Stern
Lisa Friedlander
Preston Gates Ellis & Rouvelas
Meeds LLP
1735 New York Avenue, N.W.,
Suite 500
Washington, D.C. 20006
(202) 628-1700

Attorneys for Center for Democracy and Technology

Of Counsel:
Ernest D. Miller, Law Student
Yale Law & Technology Society
Yale Law School
127 Wall Street
New Haven, CT 06520
<http://www.law.yale.edu/lawtech/>

No. of Copies rec'd 076
List ABCDE

Dated: January 27, 1999

SUMMARY

The Commission is about to set a precedent for how our society resolves law enforcement demands for surveillance capabilities in the rapidly evolving and ever-increasingly important telecommunications field. In 1994, Congress thought that it was enacting a statute that preserved a “narrowly focused” surveillance capability *and* “protected privacy in the face of increasingly powerful and personally revealing technologies.” To reach the point of enactment, parties committed to the process of balanced policymaking reached a series of compromises intended to circumscribe the role that was being granted to the FBI in the design of telecommunications systems. Specific surveillance features were excluded, most notably the ability to locate wireless phones. Privacy and innovation were made explicit design criteria, on a par with law enforcement interests. Industry was given the initial role in interpreting the Act’s requirements, subject to review by this Commission, and both were told to “narrowly interpret” those requirements. At the end, some privacy advocates in and out of Congress thought they had succeeded in creating a balanced statute that protected the public interest in effective law enforcement without jeopardizing privacy.

The Federal Bureau of Investigation apparently had a different view, and has acted ever since as if the compromises made in 1994 were irrelevant. Now with the support of the Department of Justice, the FBI has argued for inclusion of the ability to locate wireless phone users, which was such a lightning rod for privacy opposition in 1994, and which the FBI Director explicitly agreed was excluded. On a macro level, the DOJ/FBI have argued that the Act imposes no privacy obligation on carriers, even to take “technically trivial” steps that would protect privacy with no impact on law enforcement.

For the Commission to rewrite the statute as the DOJ/FBI urge would be basically to say that a binding compromise is not possible when privacy conflicts with the demands of law enforcement agencies. This precedent would have implications not only for future disputes under CALEA, but for other pending policy debates, including the encryption

issue and the question of critical infrastructure protection, two arenas where the DOJ/FBI claim to be seeking a balanced solution in language very similar to that they offered in 1994.

The central guide for CALEA interpretation should be the concept of balance – balance among the competing interests of law enforcement, privacy and innovation. Cost is also a part of this balance, both because cost was intended to serve as a constraint on law enforcement demands and because cost could divert resources from innovation. These interests (law enforcement, privacy, cost, and innovation) are clearly reflected in Section 107(b)(1) – (4) of the Act, and they constitute a guide to interpretation of the statute. The Commission must apply these four criteria reasonably and consistently when determining what is required under the Act, including determining what is required under the capability assistance provision, Section 103.

On the critical issue of packet switching, the DOJ/FBI in their December 14, 1998 comments largely agreed with CDT's factual analysis. CDT argued that carriers using emerging packet technologies (which break up communications into small packets for delivery) have an obligation under CALEA to protect privacy by distinguishing between call content and the less sensitive call-identifying information, so that the government does not intercept the former when it only has the narrower authority for the latter. In twin statements of major importance to this proceeding, the DOJ/FBI acknowledged that protecting privacy by distinguishing between call content and call-identifying information is "technically trivial" and would have no adverse impact on law enforcement.

Perversely, the DOJ/FBI go on to argue that, even though such separation is technically trivial and would be of no consequence to law enforcement, CALEA imposes no obligation on carriers to protect privacy in this way. This argument derives from the DOJ/FBI's insupportable efforts to read privacy out of CALEA altogether. What is critical to the packet issue is the DOJ/FBI's admission that protecting privacy in packet networks, as CDT has urged, is not only feasible, but would not impede law enforcement. As for the

DOJ/FBI's effort to ignore privacy, Section 103(a)(4) of the Act explicitly imposes on carriers an obligation to protect the privacy and security of communications not authorized to be intercepted. The Commission should not wait until packet technologies are more fully deployed, but should act now to clarify carriers' responsibilities so that privacy-protecting choices can be made.

The Commission's tentative decision to require carriers to design a location capability into wireless phones cannot be supported by the plain words of the Act and, further, directly contradicts the Act's legislative history. In tentatively agreeing with the carrier's "compromise" to add this capability, the Commission has turned the language of CALEA on its head, reading the statute's concern about the privacy implications of location information in wireless systems as a requirement to provide such information. In doing so, the Commission has ignored the clear legislative history, which, clarifying any ambiguity in the statute, unequivocally states that location information is not a CALEA mandate.

In evaluating the DOJ/FBI's claim for additional surveillance capabilities, and in interpreting CALEA generally, the Commission must take a reasonable overview of CALEA implementation, as the Act was intended to "preserve" a "narrowly focused" surveillance capability. The Commission must acknowledge that law enforcement's "narrowly focused" surveillance needs are well taken care of - and then some - by the industry standard. This is demonstrated by the fact that, with one exception (conference call communications to which no one suspected of criminal conduct is a party), the DOJ/FBI have no complaints at all with industry plans to ensure the government's continued ability to intercept the content of communications. The industry standard fully satisfies the purpose of CALEA insofar as the Act, in the words of the Committee reports, was intended to "insure that law enforcement can continue to conduct authorized wiretaps" in the face of rapid technological changes in the telecommunications industry. Likewise, it is clear that industry has fully committed to provide the dialing or other numeric signaling information that identifies each communication.

The DOJ/FBI have been unsatisfied, however, with this unprecedented undertaking by industry. They contend that added surveillance capabilities, the so-called punchlist, must be mandated by the Commission. Yet, with one exception, none of the punchlist items concerns dialing information and even the exception does not concern dialing information used by the local exchange carriers from whom the DOJ/FBI want to obtain it. The punchlist items are add-ons, features that might be useful to have, but they do not constitute the dialed number information covered by the pen register and trap and trace statute. Yet, the Commission has ignored the words of CALEA, tentatively concluding that certain of these punchlist items are required even though they do not fit within the plain meaning of the Act.

What is at stake here is whether the DOJ/FBI can dictate surveillance features that, at significant cost to carriers and with adverse implications for privacy, go beyond the “narrowly focused” surveillance capability Congress intended to preserve. The Commission, while it has focused up to this point largely on the DOJ/FBI perspective, correctly recognizes that understanding law enforcement’s surveillance desires does not end the inquiry into the meaning of CALEA. It is time now for the Commission to interpret Section 103 in a way that balances, as Congress intended, privacy and industry concerns against the DOJ/FBI’s demands, and enforces the compromises made in 1994.

CONTENTS

I.	TO DATE, THE COMMISSION HAS FAILED TO ADHERE TO THE PLAIN MEANING OF THE STATUTE	2
II.	GENERAL PRINCIPLES GOVERNING THIS STAGE OF THE PROCEEDING	3
A.	CALEA Does Not Guarantee One-Stop Shopping	3
B.	Cost Must Be Considered in Deciding What Is Required under Section 103	5
C.	The Factors in Sec. 107(B)(1)-(4) Are the Same Factors That Must Be Applied in Determining the Meaning of Section 103 Capability Requirements	6
D.	The Commission Must Determine What Call-Identifying Information Is Reasonably Available as a Matter Of General Obligation under Section 103, Not the FBI on a Case-by-Case Basis	7
III.	CONGRESS BELIEVED THAT PEN REGISTERS AND TRAP AND TRACE DEVICES TRADITIONALLY CAPTURED DIALED NUMBER INFORMATION ONLY	9
A.	The Pen Register/Trap and Trace Statute Is Limited to “the Numbers Dialed Or Otherwise Transmitted” and “the Originating Number”	10
B.	The Legislative History of CALEA Consistently Refers Only to Dialed Number Information	10
C.	The Courts Have Also Understood that Pen Registers and Trap and Trace Devices Collect Only Dialed Number Information	12
IV.	THE COMMISSION MUST ESTABLISH BASIC PRIVACY PRINCIPLES FOR SURVEILLANCE OF PACKET MODE COMMUNICATIONS	12
V.	LOCATION INFORMATION IS NOT REQUIRED BY CALEA	15

VI. THE PUNCHLIST ITEMS ARE NOT REQUIRED UNDER THE ACT	16
A. Post cut through dialed digits	17
B. Party hold, party join, party drop.	18
C. In band signaling	19
CONCLUSION	19

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

**REPLY COMMENTS OF THE CENTER FOR
DEMOCRACY AND TECHNOLOGY**

is unclear how law enforcement has yielded, if at all. The FBI/DOJ candidly admit that some of the punchlist items would provide information that government agencies never previously intercepted, while other items, they admit, fall outside of the scope of the Act but would nonetheless be convenient. Even the privacy-infringing capability that the FBI told Congress would not be required by the Act – the capability to locate wireless phone users – is now being sought anyway.

If the Commission accepts the DOJ/FBI view, CALEA will be transmuted into the statute Congress rejected: a one-sided mandate, interpreted by the FBI, with no privacy balance. The consequences beyond this proceeding are tremendous, for there are sure to be other punchlists as current technologies evolve and new ones emerge.

CDT has previously submitted extensive comments on the issues at stake here, on May 20, 1998, June 12, 1998, and last December 14, 1998. Throughout we refer the Commission to those earlier comments, citing them by date and page. We use the same format in citing the comments of other parties (e.g., “DOJ/FBI, 12/14/98, p. 83”).

I. TO DATE, THE COMMISSION HAS FAILED TO ADHERE TO THE PLAIN MEANING OF THE STATUTE

We urge the Commission to adhere to the plain meaning of CALEA, clarified where necessary by reference to the context of the Act and the legislative history.¹ The Commission claims to have done this. Unfortunately, on a number of points, the Commission’s tentative decisions have departed from the plain meaning of the statute, imposing on carriers mandates that are not supported by the language of the Act. Most

¹ See H.R. Rep. No. 103-827, pt.1 (1994)(House Judiciary Committee Report, hereinafter “House Report”). Unlike in many cases where there are competing House and Senate reports, a conference report, and lengthy Floor statements in both chambers, the legislative history in this case is exceptionally clear. As we have previously explained, the Senate Judiciary Committee report is identical to the House Report being cited, reflecting the close cooperation between the two Committees in drafting the legislation. S. Rep. No. 103-402 (1994). No other committees filed reports, and there was no conference, since the Senate passed the very same bill that the House passed. Thus, although some sections of the legislation changed after the Judiciary Committees acted, the Judiciary Committee reports remain the best legislative history. Many provisions ultimately enacted were unchanged from the version reported by these Committees.

egregiously, the Commission has tentatively decided to impose a wireless phone location requirement that is not only not mandated by the plain language of the Act, but which is directly excluded by its legislative history. In addition, the Commission ignored the plain meaning of the Act in its tentative decision on some of the punchlist items:

- While CALEA requires identification of each “communication,” the Commission has accepted capabilities that identify each of the “parties” to a communication.
- In further contravention of the statutory language, the Commission tentatively requires information on call attempts as well as information on communications.

Imposing design requirements on carriers that are not clearly required by the Act violates ordinary principles of statutory interpretation, which are binding upon the Commission. Broadly reading the statute to satisfy the claims of the DOJ/FBI is also clearly countermanded by the overall structure of the statute, which balances law enforcement demands against privacy and industry objections; by Congress’ clear injunction in the legislative history, which directs the Commission to narrowly interpret the Act’s capability requirements, see House Report at 23; and by prudential considerations, which weigh strongly against FCC intervention in telecommunications system design, especially where privacy is at stake.

II. GENERAL PRINCIPLES GOVERNING THIS STAGE OF THE PROCEEDING

A. CALEA Does Not Guarantee One-Stop Shopping

In judging the various proposals of the DOJ/FBI, the Commission must ask whether the contested information is available elsewhere. CALEA is premised on the notion that law enforcement should go to the place where the information sought is most readily available, even if that means going to more than one carrier to obtain a full picture of a surveillance subject’s communications activity. Under CALEA, local exchange carriers *cannot* be required to reconfigure their systems if the information sought by law enforcement is available elsewhere in the network.

This principle is reflected in Section 108(a)(1), which states that a court can issue an order enforcing CALEA against a carrier only if it finds that the “facilities of another carrier are not reasonably available to law enforcement for implementing the ... access to call-identifying information.” 47 U.S.C. §1007(a). Therefore, it would be unreasonable for the Commission to require a capability under Section 103 of the Act if a carrier will never be held responsible for providing it since the information is readily available elsewhere.

This principle is explicitly confirmed in the legislative history. The Committee reports expressly state that “[t]he bill is not intended to guarantee ‘one-stop shopping’ for law enforcement.” House Report at p. 22. The reports go on to state:

“A carrier need not insure that each individual component of its network or system complies with the requirements, so long as each communication can be intercepted at some point that meets the legislated requirements.” *Id.*, p. 23.

Given the accelerating pace of competition, it is only logical that law enforcement will have to go to various carriers to obtain a full picture of a subject’s communications activities. Congress made it clear that CALEA was not intended to undo the effects of competition, which, after all, Congress wishes to promote. The legislative history states:

“The breakup of the Bell system and the rapid proliferation of new telecommunications technologies and services have vastly complicated law enforcement’s task in that regard. The goal of the legislation, however, is not to reverse those industry trends. Indeed, it is national policy to promote competition in the telecommunications industry” *Id.*, p. 14.

Therefore, CALEA should not be interpreted to require a local exchange carrier to provide certain information if that information is readily available elsewhere in the system, albeit at somewhat greater inconvenience to law enforcement.²

² Indeed, in the case of a suspect using a calling card and multiple phones, law enforcement may find it easier to go to the long distance carrier to obtain the most useful call-identifying information.

B. Cost Must Be Considered in Deciding What Is Required under Section 103

If Congress' intent to adopt a balanced statute means anything, cost must be taken into account in determining the meaning of the Section 103 capability assistance requirements. Both privacy and industry interests, which Congress wanted protected under CALEA, entail a consideration of costs, since cost serves to constrain the enthusiasm of both government and industry for "gold-plated" surveillance features, while ignoring cost would divert resources from innovation.

Cost must be considered in determining the meaning of Section 103, since Congress clearly did not want to impose on carriers and the public costly surveillance features of limited value to law enforcement. Accordingly, cost is a consideration not only to the question of reasonable availability under the call-identifying information requirement of Section 103(a)(2), but also is a consideration throughout Section 103(a).

As the DOJ/FBI correctly point out, cost of compliance is to be considered under Section 109(b), which directs the Commission to take cost into account in determining whether to excuse a particular carrier from a CALEA obligation because it is not "reasonably achievable" for that carrier. 47 U.S.C. §1008. But contrary to the view of the DOJ/FBI, Section 109 is not the only place cost is a factor under CALEA. Section 107(b) explicitly establishes cost as a factor for the Commission to consider in setting a new "safe harbor" standard. The role of the cost factor in Section 107 is to ensure that the Commission, in setting a new industry-wide standard, does not require a capability that would be unreasonable for the industry as a whole.

Since cost is part of the Commission's Section 107 determination, cost must also be read into all of Section 103(a)'s requirements, for otherwise the Act would be requiring and the Commission would be imposing capabilities that were unachievable by most or all carriers. The DOJ/FBI's reading of the statute would force the Commission to entertain numerous individual petitions under Section 109 for relief from an interpretation of Section 103 that was unreasonable for most of the industry. The DOJ/FBI urged this time-

consuming approach once before when they claimed that the Commission could consider delay of the compliance date only upon individual petitions by individual carriers. The Commission correctly rejected the DOJ/FBI suggestion then and should also do so now. Cost obviously comes into consideration both at the safe harbor/Commission standard level and at the individual Section 109 petition stage.³

C. The Factors in Sec. 107(B)(1)-(4) Are the Same Factors That Must Be Applied in Determining the Meaning of Section 103 Capability Requirements

Congress clearly intended that the process of implementing CALEA would balance certain basic needs of law enforcement with privacy and the industry interest in ensuring that innovation proceeds unimpeded. House Report at p. 13. As we indicated, cost has implications for both privacy and industry. These four factors -- law enforcement, privacy, cost, and innovation -- are set forth in Section 107(b)(1) - (4). 47 U.S.C. §1006(b)(1) - (4). They represent the criteria that Congress wanted to be applied in interpreting CALEA.

The FBI/DOJ argue that the only function of the factors in Section 107(b)(1)-(4) is determining how the capability assistance factors must be met. The government suggests that the Commission was wrong in reading the factors as grounds for relieving a carrier of the obligation to comply with a capability requirement. We believe that there is a third, more logical reading of the statute, which is consistent with the FNPRM: the factors in Section 107(b)(1) - (4) are the factors that must be applied in determining the scope of the capability assistance requirements of Section 103. The factors (1) - (4) tell the Commission how to interpret the capability assistance requirements. They are the factors Congress assumed carriers, the FBI, and public interest organizations would apply in developing a standard that achieved CALEA's balance.

³ The DOJ/FBI argue that, if the Commission deems a capability not reasonably achievable under Section 103 because of cost, the carrier could not be obligated to provide it even if law enforcement were willing to pay the cost. This is wrong. The government can buy any capability it wants from any carrier or manufacturer under pre-existing procurement authority. Indeed, while the dispute over the adoption and implementation of CALEA has dragged on, the FBI and other law enforcement agencies have undoubtedly purchased individual capabilities for individual cases or jurisdictions.

Applying the criteria of Section 107(b) to the interpretation of the requirements in Section 103 is the only approach that yields a consistent, logical interpretation of the Act.

Congress delegated authority to the industry to interpret the capability assistance requirements. Congress did so in express disapproval of what the Administration wanted, which was a delegation of rulemaking authority to the Attorney General. House Report at pp. 26-27. Referring to the industry standards-setting process, Congress stated that “those whose competitive future depends on innovation will have a key role in *interpreting* the legislated requirements.” *Id.*, p. 19 (emphasis added).

Congress then gave the FCC the authority to review the industry’s interpretation and replace it, if needed, subject to the standards in Section 107(b)(1)-(4). These factors must be the same as the ones that Congress intended to be applied by the industry standards-setting bodies to the interpretation of the Section 103 requirements. Congress could not have intended that the FCC’s promulgation of a new standard would be based on different considerations than those guiding the initial development of the standard by industry.⁴ In determining the scope of the call-identifying requirement, the Commission on review, like the standards bodies before it in the first instance, must balance all of the factors that inform CALEA: law enforcement, privacy, industry, and cost

D. The Commission Must Determine What Call-Identifying Information Is Reasonably Available as a Matter Of General Obligation under Section 103, Not the FBI on a Case-by-Case Basis

With one exception, all of the punchlist items relate to call-identifying information. The single biggest stumbling block to the FBI’s interpretation of CALEA is the phrase “reasonably available,” which modifies the requirement to provide call-identifying information in Section 103(a)(2). 47 U.S.C. §1002(a)(2).

⁴ Similarly, Congress applied the same factors to courts’ determinations of compliance under Section 109. Congress would not have intended carriers to ignore these factors in interpreting the requirements of 103, for that would mean that industry would be adopting a standard under 103 that no one could meet and that everyone would be entitled to be excused from under Section 109.

The DOJ/FBI have a lengthy and ultimately very disruptive description of the meaning of “reasonable availability.” DOJ/FBI, 12/14/98, pp. 18 - 27. They argue that “reasonable availability” must be determined on a carrier-by-carrier, case-by-case basis.

The DOJ/FBI interpretation would eliminate all certainty from the call-identifying requirement of CALEA. This would defeat Congress’ intent that the standards process, and this Commission’s setting of a new standard if needed, would “provide[] carriers the certainty of ‘safe harbors.’” House Report at p. 26. CALEA was intended to establish uniform, minimum requirements - a nationwide baseline that would be available to law enforcement from all carriers. The DOJ/FBI interpretation would leave carriers without a safe harbor.

The DOJ/FBI proposal on “reasonable availability” would turn much of this proceeding into a hypothetical exercise. Having asked this Commission to decide that certain punchlist items are required under Section 103, the DOJ/FBI then claim that they will decide what is actually required on a carrier-by-carrier, case-by-case basis. This means that, in practice, some of the capabilities that the Commission here decides to include in the definition of call-identifying information may in fact never be required. The DOJ/FBI admit that in some platforms or networks, some punchlist items will not be reasonably available. This leaves open the possibility, by the government’s own admission, that one or more punchlist items may not be reasonably available on any platform in any network. Surely it is far better to identify those items here.

As they have so often before in this proceeding, the DOJ/FBI put forth a reading of CALEA that would leave them with the discretion to interpret the Act. They argue now that they will decide, on a case-by-case basis, what is reasonably achievable. Instead, the Commission should decide that issue, applying Congress’ specified criteria.

III. CONGRESS BELIEVED THAT PEN REGISTERS AND TRAP AND TRACE DEVICES TRADITIONALLY CAPTURED DIALED NUMBER INFORMATION ONLY

The Commission asked for comments about the type of information that has been “traditionally” available under pen register and trap and trace authorizations and whether the provision of such information in the past provides guidance for determining what call-identifying information is “reasonably available.” The history of pen registers and trap and trace devices does offer some guidance on those questions, but it may be limited.⁵

However, the language and history of the pen register and trap and trace statute is far more relevant to determining the threshold question of what the term “call-identifying information” means and what Congress intended to require by Section 103(a)(2). The record shows that Congress thought pen registers and trap and trace devices only recorded dialed numbers, and this is the capability Congress wanted to preserve under CALEA. A review of the pen register statute, of the legislative history of that statute and CALEA, and of cases describing pen register and trap and trace devices indicates that the purpose of CALEA was to preserve access to dialed number information or other signaling information corresponding to the numbers that identify an outgoing or incoming call.

This inquiry shows that over time there has been one constant: dialed number information. This is precisely what Congress intended to preserve: “the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted.” House Report, p. 21. If the Commission tries to parse the differences between various types of pen registers and trap and trace devices, and tries to trace the

⁵ First, it is clear that pen registers and trap and trace devices evolved over time. Secondly, traditionally, a law enforcement agency conducting a pen register surveillance actually obtained delivery of everything on the surveilled line, including call content. If the pen register was operated by law enforcement, the carrier simply provided a leased line from a bridge on the surveilled line - this delivered the full contents of the line to law enforcement. This was not very desirable from a privacy perspective, but there was no alternative (except placing the pen register inside company premises). Out of band signaling changed that, however, in a way that enhanced privacy. No one is arguing that pen registers should be conducted as they traditionally were. Third, a traditional pen register never captured speed dialing information, while CALEA is clearly intended to ensure that law enforcement is provided the full seven or ten digit number to which a speed dial code relates.

evolution of pen registers over time, it will find it impossible to pick a particular moment in time as the point of reference to what happened “traditionally.” There is no basis in the statute or the legislative history for picking that moment. Instead, the Commission should look to the purpose of the pen register investigation, which was Congress’ reference point.

A. The Pen Register/Trap and Trace Statute Is Limited to “the Numbers Dialed Or Otherwise Transmitted” and “the Originating Number”

The best place to start in determining what information Congress thought was traditionally available under pen registers and trap and trace devices is the statute itself authorizing pen register and trap and trace surveillance. 18 U.S.C. 3121 et seq. After all, this statutory authority is what Congress wanted to preserve by CALEA’s call-identifying information requirement. The definitions section of the pen register and trap and trace statute provides:

“(3) the term ‘pen register’ means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached ...; (4) the term ‘trap and trace device’ means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted;” 18 U.S.C. 3127.

This is the best evidence of what Congress intended to cover by the term call-identifying information.⁶

B. The Legislative History of CALEA Consistently Refers Only to Dialed Number Information

It is clear that Congress, when adopting CALEA, understood that pen register and trap and trace devices capture and record numbers identifying outgoing or incoming calls. After all, the chief law enforcement proponent of CALEA, the FBI Director, repeatedly testified

⁶ In our prior comments, we cited the language of the 1986 Senate Report on the law authorizing pen registers and trap and trace devices, the 1986 testimony of a leading expert on wiretapping, and the 1976 report of the National Wiretap Commission. CDT, 6/12/98, p. 9, all of which consistently state that pen registers record only dialed numbers and trap and trace devices identify the originating number of incoming calls. According to Professor Clifford Fishman, the pen register “does not reveal who place the call, nor who received the call, nor even whether the call was completed.” Id.

that CALEA was intended to preserve “dialed number information.”⁷ The Director made it clear that the scope of what law enforcement wanted consisted of the content of communications and “dialed number information,” meaning the telephone number dialed by a targeted facility or the telephone number of origin of an incoming call:

“Law enforcement’s requirements set forth in the proposed legislation include an ability to acquire ‘call setup information.’ This information relates to dialing type information – information generated by a caller which identifies the origin, duration, and destination of a wire or electronic communication, the telephone number or similar communication address.” Hearings, p. 33.

“What I want with respect to pen registers is the dialing information: telephone numbers which are being called, which I now have under pen register authority.” Hearings, p. 50.

In all, Freeh’s prepared testimony stated at least ten times that the requirements of the statute were intended to encompass “communications and dialing information.” Hearings, p. 24 (two references to “dialing information”), p. 27 (four references); p. 28 (four references).

In the Committee reports on CALEA, Congress expressed its understanding of what pen registers and trap and trace devices involved and it is clear that Congress though these techniques merely captured dialed number information. Once again, CDT refers the Commission to the very full explanation of “call-identifying information” in the Committee reports. House Report, p. 21. There the Committees explained their understanding of how pen register and trap and trace devices worked:

“For voice communications [call-identifying information] is typically the electronic pulses, audio tones, or signalling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier’s network. In pen register investigations, these pulses tones, or messages identify the numbers dialed from the facility that is the subject of the court order or other lawful authorization. In trap and trace investigations, these are the incoming pulses, tones or messages which identify the originating number of the facility from which the call was placed” Id.

⁷ See Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103d Cong., S. Hrg. 103-1022 (1994) (“Hearings”).

C. The Courts Have Also Understood that Pen Registers and Trap and Trace Devices Collect Only Dialed Number Information

The leading Supreme Court case on pen registers is *United States v. New York Telephone*, 434 U.S. 159 (1977).⁸ The Supreme Court there stated its understanding of what a pen register did:

“Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed – a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.” *Id.* at 167.

While the technology for these techniques has changed over time, becoming increasingly more sophisticated as one would expect, the one constant has been the collection of dialing information as well as some information showing the time when each call occurred.

IV. THE COMMISSION MUST ESTABLISH BASIC PRIVACY PRINCIPLES FOR SURVEILLANCE OF PACKET MODE COMMUNICATIONS

In a critical pair of admissions, the DOJ/FBI stated that it is “technically trivial” for carriers to withhold call content not authorized to intercept it, *and* they admit that doing so would have no negative effect on law enforcement. DOJ/FBI, 12/14/98, p. 79, fn.10, and p. 78. At the same time, however, the DOJ/FBI argue that carriers are not required to withhold content to protect privacy in this way. *Id.*, p. 79. This theory perfectly encapsulates the DOJ/FBI’s attitude towards privacy under CALEA. They have gone so far in trying to read privacy out of a statute requiring carriers to design their systems for public policy goals that they believe carriers have no obligation to take even “technically trivial” steps that would have no effect on law enforcement but would do a great deal to protect privacy.

⁸ Congress was aware of this case, for it is cited in the Committee reports on CALEA. House Report, p. 21.

This is obviously not what Congress had in mind, but it is revealing of the lack of balance that has infected the DOJ/FBI approach to CALEA.

Manufacturers, on the other hand, would have the Commission wait until it may be too late. TIA, 12/14/98, pp. 43 – 47. CDT agrees with manufacturers when they urge that the Commission not stifle the continued development of packet technologies. TIA, 12/14/98, p. 44. But nothing in CDT's proposal would stifle the development of technology or put it in a straightjacket. To the contrary, as the DOJ/FBI acknowledge, the CDT proposal is based on features "inherent" in the technology. DOJ/FBI, 12/14/98, p. 79, fn.10. CDT has presented a simple, flexible rule that takes into account the different packet protocols that exist *or may be developed in the future*: under any given protocol, whether connection-oriented or connectionless, a carrier is required to separate and provide the information that such carrier uses to route packets. Laying down this principle need not wait. Now is precisely the time to make clear that carriers must take privacy into account as they incorporate packet technology into their networks at places where it is likely to be encountered in the course of satisfying law enforcement surveillance requests.⁹

Nor is it sufficient, as the DOJ/FBI argue, to rely on law enforcement to use equipment that does not record material not authorized to be intercepted. DOJ/FBI, 12/14/98, pp. 79 – 80. That is how things were done pre-CALEA, but CALEA imposed new obligations on carriers. Just as CALEA requires carriers for the first time ever to design their systems to guarantee law enforcement access, so Section 103(a)(4) requires carriers for the first time ever to design their systems to protect privacy. Law enforcement agencies conducting pen registers in systems that do not use out-of-band signaling will still receive content and will have an obligation to minimize, but Congress decided that, when

⁹ We fully agree with manufacturers that packet technologies are subject to CALEA only when used for telecommunications, and not when they are used for "information services." TIA, 12/14/98, p. 43, n. 105. The DOJ/FBI also seem to agree with this proposition. DOJ/FBI, 12/14/98, pp. 81 – 82. In addition, we urge the Commission to recall that interexchange carriers and private networks, two of the places where packet technologies are finding their most significant applications, are not covered by CALEA. CDT, 12/14/98, p. 20.

possible, carrier systems should be designed to protect privacy at the same time they were being designed to guarantee government surveillance access.

CDT agrees fully with the point made by the manufacturers that carriers should have flexibility to comply with CALEA's requirements through different methods. TIA, 12/14/98, p. 44. But "flexibility" does not mean that carriers have an option to ignore such a basic element of protecting privacy as the distinction between call content and call-identifying information. As CDT explained in its prior comments, this distinction is at the core of the wiretap laws. CDT, 12/14/98, p. 14; CDT, 6/12/98, pp. 7-10.

Otherwise, the manufacturers largely repeat the arguments raised in their June 12, 1998 comments, to which CDT responded on December 14. CDT, 12/14/98, pp. 17 – 19. First, TIA claims that "packets of interest must be identified and captured. *Identification of particular packets for the purpose of extracting call-identifying information presents technical challenges that most carriers are not currently capable of meeting.*" TIA, 12/14/98, p. 46 (emphasis in original). As CDT pointed out in December, if carriers cannot identify and capture packets of interest, then they and law enforcement will have a much more profound problem than separating routing information from content, for carriers would not be able to comply with the requirements of CALEA Section 103(a)(1) and (2) to isolate content and call-identifying information, let alone the requirement of Section 103(a)(4) to distinguish between the two. The simple answer in a situation like the one described by TIA is that (1) law enforcement should not be going to this point in the network for surveillance assistance; and (2) CALEA does not cover the situation that TIA seems to be describing, since CALEA does not cover a carrier "that merely interconnects two other carriers."¹⁰

TIA argues that the "layered" structure of most packet-mode technologies is an added complexity. TIA, 12/14/98, p. 45. As CDT explained in its December 12 filing, it is precisely the layered nature of protocol stacks that makes it possible for carriers to

¹⁰ House Report at 23.

distinguish between call-identifying information and content. TIA concludes this point by stating, “It is important that the Commission clarify that a carrier is responsible – at most – for providing that layer of information that it reads and normally uses in routing packets.” TIA, 12/14/98, p. 46. That is precisely CDT’s position, with the added simplification that we do not object to carriers providing “lower” layers of routing information.

TIA goes on to assume, as it did in its earlier comments, that CDT is proposing that carriers be required to “extract” routing information by going through the protocol layers. *Id.* This is not CDT’s position. Contrary to TIA’s assumption, CDT is not arguing that CALEA imposes an obligation to strip off layers or conduct any analysis of anything that the carrier’s system views as content. CDT, 12/14/98, pp. 15, 19, 29

Finally, TIA argues that what constitutes “call-identifying information” will vary based on the technology being employed. TIA, 12/14/98, p. 45 n. 111. This is undoubtedly true, but it is significant that the DOJ/FBI do not consider it a problem. In fact, the DOJ/FBI state in their comments that they expect to receive different types of call-identifying information, depending on the technology. “The specific parameters that identify the ‘origin, direction, destination, or termination’ of a packet will vary depending on the data service and protocols involved. DOJ/FBI, 12/14/98, p. 83. This is not a problem that can be avoided, and it is not one that vitiates the interest in protecting privacy. As the DOJ/FBI conclude, “As long as a packet stream can be accessed, it is technically straightforward to isolate the parameters in the packet header that constitute call-identifying information, as indicated above.” *Id.*

V. LOCATION INFORMATION IS NOT REQUIRED BY CALEA

Contrary to suggestions in some of the filings, industry as a whole did not agree that location information was a CALEA requirement. Instead, as several carriers have candidly admitted in their comments, location information was not required under the Act but was included it in the J-STD anyway in a failed effort to reach an accommodation with

the FBI. US WEST, 12/14/98, p. 24; BellSouth, 5/20/98, p. 16; AT&T, 5/20/98, p. 13; Nextel, 5/20/98, n. 34.

This is something industry and the FBI cannot do: they cannot include in a CALEA standard a feature that would adversely affect privacy unless it is required by the plain meaning of the Act.

Moreover, as CDT has previously explained, the decision to require location information is inconsistent with the plain language of the statute and is directly contradicted by the legislative history. CDT, 12/14/98, pp. 4-12; CDT, 6/12/98, pp. 7-11. The Congressional hearing record is very clear: the FBI Director testified in 1994 that CALEA's call-identifying requirement "does not include any information that might disclose the general location of a mobile facility or service," Hearings at p. 29, and privacy advocates agreed, *id.* at p. 158 (testimony of Jerry Berman, "It is also important that one of the requirements that the committee has imposed is a requirement not to design ongoing location features into the ... technology ..."). The Committee reports state that CALEA requires carriers to "isolate expeditiously information identifying the originating and destination number of targeted communications, *but not the physical location of targets.*" House Report at p. 16 (emphasis added).

VI. THE PUNCHLIST ITEMS ARE NOT REQUIRED UNDER THE ACT

Much of what the DOJ/FBI seek under the guise of call-identifying information does not fit the plain meaning of the Act. The call-identifying information requirement does not include information identifying the parties to a communication, nor does it include a requirement to identify the "legs" of a call. It does not cover call attempts. Nor does it cover signaling information that is heard by to the subscriber (e.g., call waiting indicator, busy signal).

A. Post cut through dialed digits

The Commission was incorrect to conclude tentatively that post cut-through dialed digits are call-identifying information for a local exchange carrier. As we explained above, CALEA requirements must be viewed from the perspective of the carrier upon whom an order is served. The legislative history states that call-identifying information consists of “the numbers dialed or otherwise transmitted *for the purpose of routing calls through the telecommunication carrier’s network*,” House Report, p. 21 (emphasis added), not through the network of another carrier. From the perspective of a LEC, post cut through dialed digits are not dialing or signaling information used to process calls; they are content.

Under Section 107(b)(1), the approach proposed by the government is not cost effective, especially since the government can obtain what it wants from the long distance carrier that uses the sought-after digits for call processing. The government claims that this is too hard. Sometimes it is harder, sometimes it is not. Consider the following scenario. The target uses an AT&T long distance calling card to make long distance calls. The card allows him to place long distance calls from any hardwire phone, any wireless phone, and any pay phone. The target who starts his day in Washington uses Bell Atlantic, then proceeds in a cab to Dulles using a cell phone with a different carrier. Then, upon reaching Dulles, uses pay phone not provided by Bell Atlantic. Under the DOJ/ FBI scenario, government would have to go to all three carriers to obtain dialed number information. Under the CDT scenario, law enforcement would have to go to only one: AT&T.

Section 107(b)(2) requires implementation of CALEA to “protect the privacy and security of communications not authorized to be intercepted.” The approach proposed by DOJ/FBI clearly and admittedly infringes on the privacy of communications not authorized to be intercepted. The DOJ/FBI admit that this punchlist item would allow the government to intercept content under a pen register order. The DOJ/FBI also admit that it is not possible for carriers to distinguish between post cut through dialed digits used by a downstream carrier for call processing and those that are content even at the termination

point of the call. DOJ/FBI, 12/14/98, p. 67. DOJ/FBI argue that law enforcement's obligation to minimize under the wiretap law is sufficient to protect privacy, but if Congress had thought that privacy was adequately protected under the wiretap laws, it would not have written a separate privacy requirement into CALEA.

B. Party hold, party join, party drop

The FNPRM ignores the plain meaning of the statute in its conclusion that party hold, party join and party drop messages identify "the temporary origin, temporary termination or re-direction of a communication." However, the concepts of "temporary" origin and "temporary" termination appear nowhere in the statute. To the contrary, they are contradicted by the plain meaning of the statute. When a party drops off a call that is continuing, the communication does not terminate. When a party joins a communication in progress, the call does not originate. And of course, the same is true of party hold: a communication is not terminated when a party is put on hold and is not originated when the party is brought back in from having been on hold.

The DOJ/FBI originally claimed that this capability would allow the government to identify the "origin, direction, destination or termination" of "each leg" of a call. Joint Petition, ¶ 78. The "each leg" concept was made out of whole cloth. Congress did not use the "each leg" concept, nor does the legislative history contain any intention that call-identifying information would apply to each leg of a communication.

More recently, the DOJ/FBI claim that this capability is necessary to identify the parties to a communication. This too is not covered by CALEA, as the Act only requires carriers to be able to identify communications.¹¹

The J-STD has correctly interpreted CALEA on this point. It recognizes that a conference call may have more than one point of origin and more than one point of

¹¹ The DOJ/FBI claim that this information is necessary for law enforcement to know who is hearing what in the course of a conversation. A search of the legislative record does not uncover any instance in which they ever mentioned this in the hearings on CALEA. Not too long ago, the government claimed with equal certainty that it was necessary and required under CALEA for carriers to separate onto a distinct delivery channel the content for each speaker, so that the government could tell who was saying what.

termination, since there may be multiple parties. So the J-STD will provide call-identifying information on each of the parties that are brought into the call. It will not indicate when they drop off or are put on hold. It will indicate when the call ends.

The Commission has accepted the FBI's invitation to interpret the statute as if it required "party-identifying information." Congress could have imposed a requirement on the carriers to identify the parties to a communication, and it could have imposed a requirement on carriers to identify each leg of a communication, but it did not do so. Congress apparently did not believe that this level of specific information about activity inside a call was necessary to identify the communication.

C. In band signaling

The Commission has again gone beyond the plain meaning of the statute in concluding that in band signaling is required as part of call-identifying information. Much of what the DOJ/FBI seek under this punchlist item is not covered by the plain language of CALEA, for CALEA only requires call-identifying information on "communications," while most of this punchlist item concerns call attempts. When a call attempt is unsuccessful, the DOJ/FBI want to know why it was unsuccessful -- why did a communication not occur, was it because the calling party received a busy signal, was it because the phone rang but nobody on the other end answered?¹² The FBI also wants a incoming call indicator. This is another effort to identify a call attempt. If the call is completed, the J-STD will identify it. The J-STD does not provide law enforcement with the number of a calling party on a call that was not completed.

CONCLUSION

It is entirely understandable that the Commission is eager to assist the FBI in carrying out its important public safety obligations. Thus far, the Commission seems to

¹² Under the J-STD, the government will actually get the dialed numbers identifying call attempts. This is not covered by CALEA, but we do not suggest here that it is prohibited either.

have decided that if it is unclear whether CALEA requires a certain capability, it should be required if the DOJ/FBI show that it would be useful. However, Congress adopted quite a different approach in CALEA. Congress required a balance between law enforcement interests and the considerations of privacy and industry. The concept of balance means that capabilities arguably falling within the scope of the Act are not mandated if they would have adverse cost, innovation or privacy concerns, even if they would be useful to law enforcement, so long as the core surveillance capability is preserved. If there is a doubt about whether something is mandated under CALEA, it should be excluded from coverage.

While pushing the Commission to adopt a broad and loose reading of the legislation, the DOJ/FBI have tried to focus the Commission on a narrow range of issues -- the utility of the individual punchlist items. They argue that each item is necessary to the future of law enforcement operations.

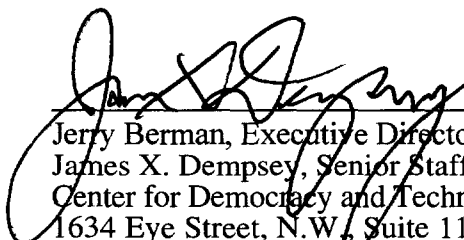
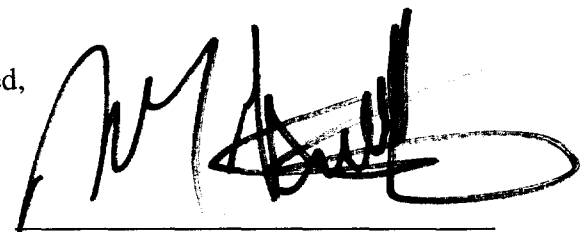
Contrary to the implications of the DOJ/FBI's arguments, law enforcement surveillance has been and will continue to be vastly enriched by the digital revolution, especially given industry's commitment in the J-STD to guarantee law enforcement access to the content of any suspect's communications. Any objective look at communications today, and communications in the future, would lead to the conclusion that there is more information more easily available to law enforcement interception than ever before. A criminal using a wireless phone is far easier to surveil than one with a pocket full of change and a choice of pay phones. Calling cards and network intelligence make it possible to locate users anywhere in the country. To the extent that many people use e-mail as a substitute for telephone calls, e-mail is far friendlier to surveillance since it is not ephemeral, but remains in storage, often even after being read "deleted" by the intended recipient. The ubiquity of telecommunications makes far more information available. Law enforcement undoubtedly has been successful in exploiting the surveillance potential of the new technology. And the J-STD will provide the government a sophisticated, integrated surveillance capability to even more readily capture and analyze that data.

One of the most extraordinary aspects of the DOJ/FBI's attempt to enlist this Commission in dictating specific surveillance demands to industry is that none of the issues at stake here touches upon the government's ability to intercept communications of suspected criminals. The industry has already fully committed to ensure that the government will have the ability to easily intercept the communications of criminals.

Why then are the parties fighting so hard over these issues? The companies are fighting because the punchlist items are expensive. Privacy groups are fighting because we are concerned with the efforts of the FBI through these specific punchlist items to build up the richness of the signaling channel, a channel to which the government has access under a minimal standard. The FBI is fighting, we assume, because they believe that the punchlist items would be truly useful. But why is the FBI fighting so hard, over what by any standard are incremental changes in what it receives? Why was it willing to suffer a delay of CALEA compliance for what at some level appear to be incremental capabilities?

The answer is that all parties are looking to the future. It is a question of precedent. If the government can convince the Commission to mandate these punchlist items, the push and pull of the standards-setting process on future technologies will be skewed. If the Commission adopts a broad interpretation of CALEA, and mandates some or all of the punchlist items, the FBI's position will be substantially strengthened. In essence, CALEA will be rewritten, to give the FBI what it has always wanted and which Congress refused to give it: the power to dictate surveillance features.

Respectfully submitted,


 Jerry Berman, Executive Director
 James X. Dempsey, Senior Staff Counsel
 Center for Democracy and Technology
 1634 Eye Street, N.W., Suite 1100
 Washington, D.C. 20006
 Suite 500
 (202) 637-9800
<http://www.cdt.org>

 Martin L. Stern
 Lisa Friedlander
 Preston Gates Ellis & Rouvelas
 Meeds LLP
 1735 New York Avenue, N.W.,
 Washington, D.C. 20006
 (202) 628-1700

Attorneys for Center for Democracy and Technology

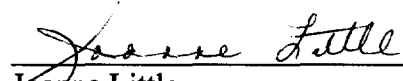
Of Counsel:

Ernest D. Miller, Law Student
Yale Law & Technology Society
Yale Law School
127 Wall Street
New Haven, CT 06520
<http://www.law.yale.edu/lawtech/>

Dated: January 27, 1999

CERTIFICATE OF SERVICE

I, Joanne Little, do hereby certify that copies of the forgoing Reply Comments of the Center for Democracy and Technology have been served on the persons listed below via first class mail delivery on this 27th day of January, 1999.


Joanne Little

* BY HAND

*The Honorable William E. Kennard
Federal Communications Commission
The Portals
445 12th St., SW, 8B201
Washington, DC 20554

*The Honorable Susan Ness
Federal Communications Commission
The Portals
445 12th St., SW, 8B115
Washington, DC 20554

*The Honorable Gloria Tristani
Federal Communications Commission
The Portals
445 12th St., SW, 8C302
Washington, DC 20554

*The Honorable Harold Furchtgott-Roth
Federal Communications Commission
The Portals
445 12th St., SW, A8302
Washington, DC 20554

*The Honorable Michael Powell
Federal Communications Commission
The Portals
445 12th St., SW, 8A204A
Washington, DC 20554

*Paul Misener
Federal Communications Commission
The Portals
445 12th St., SW, 8-302
Washington, DC 20554

*Peter A. Tenhula
Federal Communications Commission
The Portals
445 12th St., SW, 8-A204A
Washington, DC 20554

*Magalie R. Salas
Office of the Secretary
Federal Communications Commission
The Portals
445 12th St., SW
Washington, DC 20554

*Ari Fitzgerald
Federal Communications Commission
The Portals
445 12th St., SW, 8-B201
Washington, DC 20554

*Karen Gulick
Federal Communications Commission
The Portals
445 12th St., SW, 8C302
Washington, DC 20554

***Daniel J. Connors, Jr.**
Federal Communications Commission
The Portals
445 12th St., SW, 8B115
Washington, DC 20554

***Thomas J. Sugrue**
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, NW – Room 5002
Washington, DC 20554

Dale Hatfield
Federal Communications Commission
Office of Engineering & Technology
2000 M Street, NW, Room 230
Washington, DC 20554

Rebecca Dorch
Federal Communications Commission
Office of Engineering & Technology
2000 M Street, NW, Room 230
Washington, DC 20554

***Lawrence Petak**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554

***Charles Isman**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554

The Honorable Janet Reno
Attorney General
Department of Justice
Constitution Avenue & 10th Street, NW
Washington, DC 20530

Douglas N. Letter, Esquire
Appellate Litigation Counsel
Civil Division
Department of Justice
601 D Street, NW – Room 9106
Washington, DC 20530

Larry R. Parkinson, Esquire
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Thomas Wheeler, President
Cellular Telecommunications Industry
Assoc.
1250 Connecticut Avenue, NW
Suite 200
Washington, DC 20036

Roy Neel, President
United States Telephone Association
1401 H Street, NW – Suite 600
Washington, DC 20005

***Jim Burtle**
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554

Stephen W. Preston
Deputy Assistant Attorney General
Civil Division
Department of Justice
601 D Street, NW
Washington, DC 20530

The Honorable Louis J. Freeh, Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Grant Seiffert
Director of Government Relations
Telecommunications Industry Association
1201 Pennsylvania Avenue, NW
Suite 315
Washington, DC 20004

Jay Kitchen, President
Personal Communications Industry Assoc.
500 Montgomery Street – Suite 700
Alexandria, VA 22314

Stewart Baker
Steptoe & Johnson
1330 Connecticut Avenue, NW
Washington, DC 20036

Douglas I. Brandon
AT&T Wireless Services Inc.
1150 Connecticut Avenue, NW
4th Floor
Washington, DC 20036

Catherine Wang
Swidler & Berlin
3000 “K” Street, NW – Suite 300
Washington, DC 20007

*Tim Maguire
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, NW – Room 8038
Washington, DC 20554

*David Sylvar
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554

Dean L. Grayson
LUCENT Technologies Inc.
1825 “Eye” Street, NW
Washington, DC 20006

*ITS
1231 20th Street, NW
Washington, DC 20036

*Kimberly Parker
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, NW – 7th Floor
Washington, DC 20554

Elaine Carpenter
Aliant Communications, Inc.
1440 M Street
Lincoln, NE 68508

Michael W. Mowery
Air Touch Communications, Inc.
2999 Oak Road, MS 1025
Walnut Creek, CA 95596

James F. Ireland
Theresa A. Zeterberg
Cole, Raywind & Braverman, LLP
1919 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006

Andre J. Lachance
GTE Service Corporation
1850 M Street, NW
Suite 1200
Washington, DC 20036

Mark C. Rosenblum
Ava B. Kleinman
Seth S. Gross
295 North Maple Avenue
Room 3252F3
Basking Ridge, NJ 07920

John T. Scott, III
Crowell & Moring LLP
1001 Pennsylvania Avenue, NW
Washington, DC 20004

Pamela J. Riley
David A. Gross
Air Touch Communications, Inc.
1818 N Street, N.W.
Suite 320 South
Washington, DC 20036

Glenn S. Rabin
ALLTEL Corporate Services
655 15th Street, NW
Suite 220
Washington, DC 20005

John F. Raposa
Richard McKenna
GTE Service Corporation
600 Hidden Ridge, HQE03J36
PO Box 152092
Irving, TX 75015-2092

William L. Roughton, Jr.
PrimeCo Personal Communications
601 13th Street, NW
Suite 320 South
Washington, DC 20005

Douglas I. Brandon
AT&T Wireless Services
1150 Connecticut Avenue, NW
4th Floor
Washington, DC 20036

M. Robert Sutherland
Theodore R. Kingsley
Bell South Corporation
1155 Peachtree Street, NE
Suite 1700
Atlanta, GA 30309-3610

Stephen O. Kraskin
Sylvia Lesse
Joshua Seidemann
Kraskin, Lesse & Cosson, LLP
2120 L Street, NW
Suite 520
Washington, DC 20037

Robert Vitanza
SBC Communications, Inc.
15660 Dallas Pkwy. – Suite 1300
Dallas, TX 75248

Katherine Marie Krause
Edward M. Chavez
1020 19th Street, NW
Washington, DC 20036

Christine M. Gill
McDermott, Will & Emery
600 13th Street, NW
Suite 1200
Washington, DC 20005-3096

David L. Nace
Lukas, McGowan, Nace & Gutierrez
1111 19th Street, NW
Suite 1200
Washington, DC 20036

Stephen J. Rosen
Wiley, Rein & Fielding
1776 K Street, NW
Washington, DC 20006-2304

James D. Ellis
Robert M. Lynch
Durward D. Dupre
Lucille M. Mates
Frank C. Magill
SBC Communications, Inc.
One Bell Plaza – Suite 3703
Dallas, TX 75202

William T. Lake
John H. Harwood II
Samir Jain
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, NW
Washington, DC 20037-1420

Stephen L. Goodman
Halprin, Temple, Goodman & Sugrue
1100 New York Avenue, NW
Suite 650 East
Washington, DC 20005

Emilio W. Cividanes
Piper & Marbury LLP
1200 19th Street, NW
Washington, DC 20036-2430

Peter M. Connolly
Koteen & Naftalin, LLP
1150 Connecticut Avenue, NW
Suite 1000
Washington, DC 20036-4196

Paul G. Madison
Kelley, Drye & Warren LLP
1200 19th Street, NW
Suite 500
Washington, DC 20036

L. Marie Guillory
NTCA
2626 Pennsylvania Avenue, NW
Washington, DC 20037

Lisa M. Zaina
OPASTCO
21 Dupont Circle, NW
Suite 700
Washington, DC 20036

Kevin C. Gallagher
360 Communications Company
8725 Higgins Road
Chicago, IL 60631

Lawrence R. Krevor
NEXTEL Communications, Inc.
800 Connecticut Avenue, NW
Suite 1001
Washington, DC 20006-2720

Alane C. Weixel
Covington & Burling
1201 Pennsylvania Avenue, NW
P. O. Box 7566
Washington, DC 20044-7566

Barbara J. Kern
Ameritech Corporation
4H74
2000 Ameritech Center Drive
Hoffman Estates, IL 60196

Richard J. Metzger
Association for Local
Telecommunications Services
888 17th Street, NW – Suite 900
Washington, DC 20006

Colette M. Capretz
Fisher, Wayland, Cooper, Leader &
Zaragoza
2001 Pennsylvania Avenue, NW
Suite 400
Washington, DC 20006-1851

Henry M. Rivera
Shook Hardy & Bacon
Market Square West
801 Pennsylvania Avenue, NW
Suite 600
Washington, DC 20004-2615

Cheryl Tritt
Morrison & Forerster LLP
2000 Pennsylvania Avenue, NW
Suite 5500
Washington, DC 20006-1812

John Pignataro
Senior Technical Advisor NYPD
Ft. Totten Building 610
Bayside, NY 11359